Department of Administrative Services
Enterprise Information Strategy and Policy Division
955 Center Street NE, Rm. 470
Salem, OR 97301
Phone: (503) 378-3175
Fax: (503) 378-3795

September 15, 2009

Attorney General John Kroger
Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096

Dear Mr. Kroger,

Over the past decade or more, the Legislature has enacted statutes that have created numerous exceptions to the public records law. Those exceptions have created impediments to data sharing between government agencies at every level. The vision of the Governor's Oregon Geographic Information Council is to enable increased sharing of geographic data to improve government decision making at all levels. On behalf of the Council, I ask the Attorney General's Office to broaden the ongoing review of the Oregon public records laws to address impediments to data sharing between government agencies. The Council and my office would be pleased to assist in any way needed.

Actions by government agencies that save lives, protect property, conserve the environment, and ensure sustainable development have a crucial element in common: Success depends on reliable, accurate, timely information. Today, many decisions are based on the best available data, which can be limited and therefore introduce uncertainty. Often, required data is not available when needed or is inadequate to support decisions. Ideally, data should be collected only once and shared with other government agencies. This would improve the efficiency of government and decision making processes.

Confidentiality of data and information is an issue affecting many federal, state, and local governments as they attempt to use information systems in making informed choices leading to good policy and decisions. Government is buffeted by the competing demands for public information and the need to protect the confidentiality of information.

Confidentiality restrictions lead to duplication of effort and increased government cost when all governmental budgets are under intense pressure for increased efficiencies. Governmental entities are collecting information and creating databases already collected and created by other entities simply because one or all cannot share their information. Government has the ability to analyze and present data and information in ways that were not thought of a few years ago. Yet, most, if not all statutes governing confidentiality and the sharing of information were written before decision-making tools such as Geographic

Information Systems (GIS), Modeling, Impact Analysis, and Performance Measurement were developed.

GIS, because of its ability to combine computer based mapping, database management systems, and powerful statistical and data analysis systems, complicates the confidentiality issue even more. Is a dot on a map confidential information? Scale, statistics, data categorization, mapping methods, and aggregation methods all can impact whether GIS data violates confidentiality requirements.

Currently, there are three approaches to GIS-related confidentiality in Oregon government:

- Share everything;
- Share only with specific partners for specific purposes; and
- Share nothing.

Some government agencies have websites where the public can view detailed information such as property tax assessments, water rights, or hazardous waste sites. Other agencies post only aggregate or summarized data to their websites.

Where possible, information should be shared between government entities and with the public. Statutes and policies that prevent sharing of information in cases where harm to the individual is not an issue, or where the right to confidentiality can still be protected, should be examined and if necessary, modified or eliminated. Again, if there is any way in which my office or the Council can assist your office in its examination of the Oregon public records laws related to data sharing between government agencies, please let me know.

Sincerely,

Dugan Petty, State CIO
Chair, Oregon Geographic Information Council
DAS/Enterprise Information Strategy & Policy Division
955 Center St. NE
Salem, OR 97301
503-378-3175

Cc: Scott Harra, Director
Oregon Department of Administrative Services

David Leith, Assistant Attorney General
Oregon Department of Justice

MEMORANDUM

TO: David Leith
Associate Attorney General
Oregon Department of Justice

FROM: Lonn Hoklin
Public Affairs Manager
Oregon Department of Administrative Services

DATE: September 3, 2009

RE: Suggested amendments to the state Public Records Law

In answer to your request of last June, we offer the following suggestions and considerations that relate to amending Oregon's Public Records Law. At DAS, we believe that access to public information is an important right of all citizens. Nonetheless we bear an obligation to give equal attention to protecting confidential and personal information. We welcome the opportunity to work with your team in drafting appropriate changes to the law.

Note: DAS Risk Management requests an opportunity to address any proposed amendments that affect its handling of public information. As you know, Risk Management plays an important role in protecting the state from liability and in safeguarding individuals' confidential information in documents that relate to lawsuits, tort claims and other actions.

Geospatial Enterprise Office

The Geospatial Enterprise Office (DAS Enterprise Information Strategy and Policy Division) has begun to engage its many state and local stakeholders and partners on issues involving the Public Records Law. Over the years, numerous revisions to the law have occurred with little or no attention to the overall consequences for the multitude of jurisdictions that rely on data gathered through geographic information systems.

This piecemeal approach has generated many conflicts that complicate data-sharing among jurisdictions, or make it downright impossible. Recent exceptions to Public Records Law requirements for certain classes of individuals have prompted many local officials to refuse to share information with other jurisdictions, primarily because of concerns over liability, both personal and professional.

The process of formulating amendments that pertain to geographic information systems will proceed on a separate track, involving input from state and local stakeholders. We will notify you of any developments in this area.

Enterprise Security Office

The need for transparency and access to public information in state government is as an important right of all citizens. Every agency bears an obligation to protect that right. Balanced against the "right to know," however, is the requirement to ensure adequate and appropriate protection of confidential information. A review of the current Oregon Public Records Law reveals areas that do not adequately ensure the *security* of state information and systems. Following are the DAS Enterprise Security Office (ESO) concerns and recommended revisions.

Specific ORS Sections of Concern:

ORS 192.501 - **Public records conditionally exempt from disclosure** – The following public records are exempt from disclosure under ORS 192.410 to 192.502 unless the pubic interest requires disclosure in the particular instance.

ORS 192.501 (22) - Records or information that, if disclosed, would allow a person to:
(b) Identify those areas of structural or operational vulnerability that would permit unlawful disruption, or interference with, services; or
(c) Disrupt, interfere with or gain unauthorized access to public funds or to information processing, communications, or telecommunications systems, including the information contained in the systems, that are used or operated by a public body;

(23) Records or information that would reveal or otherwise identify security measures, or weaknesses or potential weaknesses in security measures, taken or recommended to be taken to protect:

(a) An individual;
(b) Buildings or other property
(c) Information processing, communications or telecommunications systems, including the information contained in the systems;

ORS 192.502 – **Other public records exempt from disclosure** – The following public records exempt from disclosure under ORS 192.410 to 192.505:
(33) Information about review or approval or programs relating to the security of:

(b) Telecommunications systems, including cellular, wireless or radio systems
(c) Data transmissions by whatever means provided. [CSA1]

Background:

The State of Oregon is responsible for protecting any confidential information it obtains, shares, manages, transmits, stores, and ultimately discards. ORS 182.122 (Information Systems Security) and ORS 646A.600 to 646A.628 (Oregon Consumer Identity Theft Protection Act) provide specific direction to state agencies, in addition to the enterprise information security policies, standards, and procedures adopted by the Department of Administrative Services.

Information identified in ORS 192.501 (22) (a), (b) and (c) and (23) (a), (b), (c), and (d) is not adequately protected. [Section (23) (d) focuses on the operations of the Oregon State Lottery that are subject to several statues, both state and federal; this document does address provisions that relate to the Lottery].

Determining whether to disclose is a "balancing test" that agencies perform to weigh the need for confidentiality versus the public's interest in disclosure. The test often results in inconsistent application of the law and the potential release of information that should be protected.

The same generally holds true with respect to records covered under ORS 192.502. The statute, however, declares that these records are exempt from disclosure, since the legislature has determined that the need for confidentiality of those types of records outweighs the public's interest in disclosure.

Concerns:

Both ORS 192.501 and ORS 192.502 contain "exemptions" from disclosure for certain public records. But these statutes do not "prohibit" disclosure. Agencies may voluntarily reveal information that is exempt from disclosure. Records covered in both ORS 192.501 and ORS 192.502—records that agencies may disclose—represent a security threat.

ORS 192.501 (23), for example, focuses on records that would reveal security measures or weaknesses. Exposure of such information could occur through security audits, assessments, and remediation plans. Release of such information to the public would jeopardize protection of state-owned information and systems, thereby compromising personal information that should clearly remain confidential. Publicly available documents that reveal security weaknesses, detail network schemas, or enable unauthorized access to systems would provide a roadmap for someone with malicious intent. Material with this type of information and detail should be available only to those who have a "right and need to know," and only if they sign non-disclosure/confidentiality agreements.

Recommendation:

1. ORS 192.502 Section (33) should be revised to include item (d) (below)

(33) Information about review or approval of programs relating to the security of:
(a) Generation, storage or conveyance of:
(A) Electricity;
(B) Gas in liquefied or gaseous form;
(C) Hazardous substances as defined in ORS 453.005 (7)(a), (b) and (d);
(D) Petroleum products;
(E) Sewage; or
(F) Water.
(b) Telecommunication systems, including cellular, wireless or radio systems.
(c) Data transmissions by whatever means provided.
(d) *Information system security vulnerabilities that could compromise information systems.*

State Procurement Office

The State Procurement Office recommends consideration of the following issues during the review of the Public Records law.

The Public Record law should address the following issues:

1. While a solicitation process is under way, the state should not immediately fulfill public records requests that involve the project or contract for which it is soliciting proposals or bids. Information should become available for review only after the state issues the *intent to award.* The state should not release any bids or proposals received in response to a cancelled solicitation until determining that the solicitation will not be re-released. If the solicitation is to be re-released, the proposals or bids from the cancelled solicitation should only be available after the intent to award has been issued for the subsequent solicitation.

2. The law should prohibit selling for financial gain any information or documents obtained through public records requests. Some companies sell winning proposals to their subscribed membership lists.

3. In several instances, news media have requested a waiver of fees that SPO has rejected on the advice of DOJ. It would be helpful if the Public Records Law provides that news media requests are not subject to fee waiver as outlined in ORS 192.440(5) and (6).

4. The law should include guidelines in handling requests that deal with copyrighted material.

5. The law should exempt trade secrets from the Public Records Law. The law should require, however, that a proposal must clearly indicate which material constitutes a trade secret (i.e., an entire proposal cannot be a trade secret).

The following issues may not to be appropriate for resolution in statute, but may deserve to be addressed in policy.

DAS Public records requests fees:

   a. Fees for copying should receive periodic review and evaluation.

   b. A review of public records sometimes requires SPO staff person to supervise the review for hours at a time. SPO cannot leave these files unattended and unguarded. Policy should authorize SPO to charge a "supervision fee."

   c. Policy should address charging appropriate fees for downloads of electronic information.